FortiAuthenticator - Release Notes

Version 6.0.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

2021-08-19
FortiAuthenticator 6.0.2 Release Notes
23-602-566029-20210819

TABLE OF CONTENTS

Change log

Date	Change Description
2019-06-20	Initial release.
2021-08-19	Updated Product integration and support on page 11.

FortiAuthenticator 6.0.2 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.0.2, build 0041.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit:

https://docs.fortinet.com/product/fortiauthenticator/

Special notices

TFTP boot firmware upgrade process

Upgrading FortiAuthenticator firmware by interrupting the FortiAuthenticator boot process and installing a firmware image from a TFTP server erases the current FortiAuthenticator configuration and replaces it with factory default settings.

Monitor settings for GUI access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the GUI to be viewed properly without the need for scrolling.

Before any firmware upgrade

Save a copy of your FortiAuthenticator configuration before upgrading the firmware. Go to **System > Dashboard > Status** and select **Backup/Restore > Download Backup File** to backup the configuration.

After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

What's new

FortiAuthenticator version 6.0.2 is a patch release. There are no new features. See Resolved issues on page 15 and Known issues on page 17 for more information.

Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Hardware and VM support

FortiAuthenticator 6.0.2 supports:

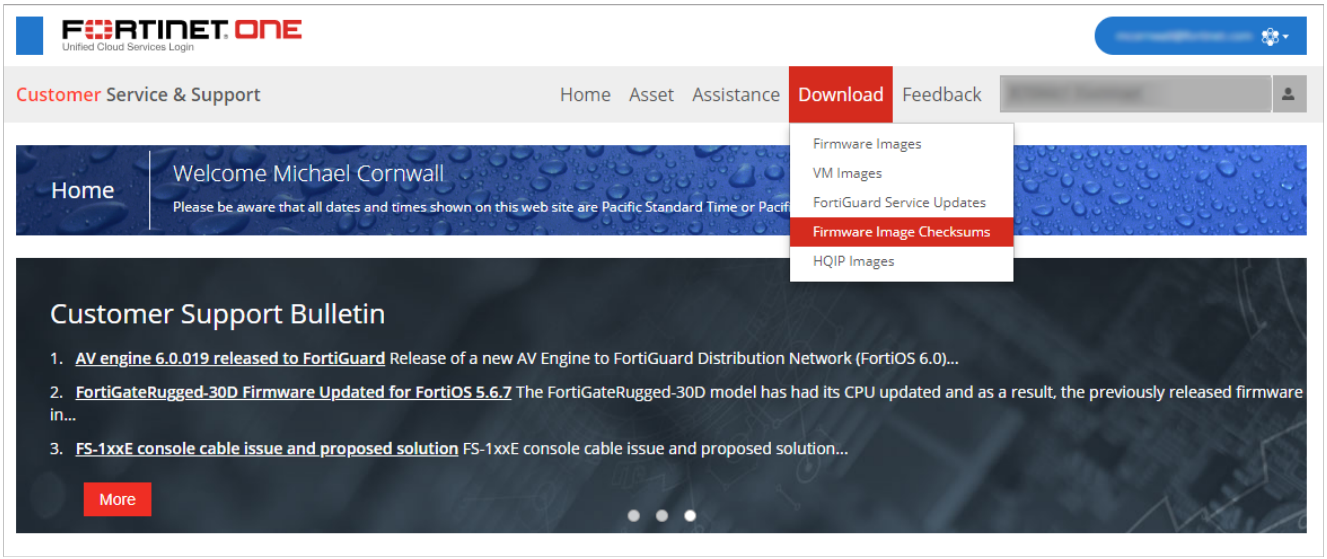
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, and Azure)

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the Fortinet Support website.

Customer service and support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from FortiAuthenticator 4.x/5.x/6.0.x

FortiAuthenticator 6.0.2 build 0041 officially supports upgrade from all versions of FortiAuthenticator 4.x, 5.x, and 6.0.x.

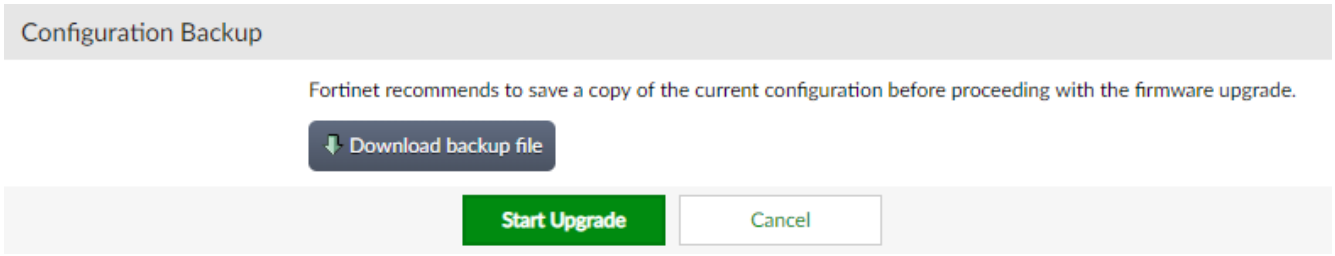
Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Go to **System > Dashboard > Status**.
5. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
6. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
7. Select **OK** to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.

Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

Product integration and support

Web browser support

The following web browsers are supported by FortiAuthenticator 6.0.2:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 42
- Mozilla Firefox version 67
- Google Chrome version 74

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator 6.0.2 supports the following FortiOS versions:

- FortiOS v6.4.x
- FortiOS v6.2.x
- FortiOS v6.0.x
- FortiOS v5.6.x
- FortiOS v5.4.x

Fortinet agent support

FortiAuthenticator 6.0.2 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.3
- FortiAuthenticator Agent for Outlook Web Access 1.6
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

Virtualization software support

FortiAuthenticator 6.0.2 supports:

- VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM and AWS)
- Microsoft Azure

Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See FortiAuthenticator VM on page 13 for more information.

Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS).

FortiAuthenticator VM

FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator virtual machine (VM) system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported VM environment. For details, see the FortiAuthenticator VM Install Guide.

VM requirements

Virtual machine	Requirement
VM form factor	Open Virtualization Format (OVF)
Virtual CPUs supported (minimum / maximum)	1 / 64
Virtual NICs supported (minimum / maximum)	1 / 4
Storage support (minimum / maximum)	60 GB / 16 TB
Memory support (minimum / maximum)	2 GB / 1 TB
High Availability (HA) support	Yes

FortiAuthenticator VM sizing guidelines

The following table provides FortiAuthenticator VM sizing guidelines based on typical usage. Actual requirements may vary based on usage patterns.

VM sizing guidelines

Users	Virtual CPUs	Memory	Storage
1 - 500	1	2 GB	1 TB
500 to 2,500	2	4 GB	1 TB
2,500 to 7,500	2	8 GB	2 TB
7,500 to 25,000	4	16 GB	2 TB
25,000 to 75,000	8	32 GB	4 TB

Users	Virtual CPUs	Memory	Storage
75,000 to 250,000	16	64 GB	4 TB
250,000 to 750,000	32	128 GB	8 TB
750,000 to 2,500,000	64	256 GB	16 TB
2,500,000 to 7,500,000	64	512 GB	16 TB

FortiAuthenticator VM firmware

Fortinet provides FortiAuthenticator VM firmware images in two formats:

- **.out**
  Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip**
  Use this image for new VM installations. It contains a deployable OVF virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, https://www.fortinet.com/products/identity-access-management.html#models-specifications.

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
565706	Upgrade kernels to address TCP SACK vulnerabilities: CVE-2019-11477, CVE-2019-11478, and CVE-2019-11479.
548689	FortiAuthenticator should not delete a revoked local service certificate until it has expired.
524382	Increase the timeout limit for RADIUS requests to 60 seconds.
560427	If a custom RADIUS dictionary with a duplicated attribute number is uploaded to FortiAuthenticator, the GUI becomes inaccessible.
563148	Occasionally, FortiToken Mobile push notifications are accepted only after a second approval.
538216	FortiAuthenticator FSSO service can be unstable due to crashing DC agent daemon.
561938	For local users, FortiAuthenticator should not allow the use of passwords over 64 characters.
561200	The IdP metadata file contains an incorrect SP certificate format which causes SAML authentication failure.
560326	Users who have logged into a computer running Windows 8.1 or Windows 10 using a Microsoft Account continue to have the ability to log in with the account despite enabling the FortiAuthenticator Windows Agent option to disable Microsoft Providers.
563820	When PCI is enabled, attempting to log into the GUI with a username that does not exist causes FortiAuthenticator to crash.
561934	In the GUI banner, replace the build label with the FortiAuthenticator model number.
557353	Occasionally, FortiAuthenticator widgets fail to load.
558329	On the login page, relocate "Sign in as different user" link beneath the login box.

Common Vulnerabilities and Exposures

FortiAuthenticator is no longer vulnerable to the following CVE-Reference(s):

- CVE-2019-11477
- CVE-2019-11478
- CVE-2019-11479

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
555180	Push notification certificates are not restored to the disk following a model conversion.
526202	FortiAuthenticator does not check if the signature of a CSR is valid when processing it during a SCEP enrollment request.
538059	Importing an ECDSA-signed certificate and key causes an error.
544851	Unable to re-enable HA from the CLI if HA was disabled from the GUI on the backup device.
528352	Unable to configure HA role and priority from the CLI on a load-balancing device that has HA disabled.
546764	The use of non-ASCII characters in replacement messages causes the URL in email messages to render incorrectly.
478985	The FortiAuthenticator Windows Agent does not always locate the domain name, and users are not able to login.
524131	There is a multisecond delay between queuing and sending of push notifications.
468513	Excluding a user from SSO causes the FSSO server to exit and not recover.
540932	FSSOMA nested group search fails if nested via the primary group.
541043	SAML authentication with Azure UUID mapping does not include SSO group for the user as expected.
555320	When using device only (MAC address) authentication, the guest portal time schedule is ignored.
482900	User registration through a guest portal requires the approver to enable RADIUS authentication first.
558797	Users assigned an admin profile with full read and write permissions are unable to access **Authentication > Guest Portals > General**.
532604	The **Social Login Users** list displays "unknown" in the user column.
530392	Unable to log into a guest portal with a social user account if the account has expired. **Workaround**: From **Authentication > User Account Policies > General**, enable **Automatically purge disabled user accounts** and set the frequency to **Hourly**. This removes all expired accounts.
543791	When a users audit report is generated, the "last used" and "created" columns contain incorrect data for LDAP users.

Bug ID	Description
510931	The connection status displayed for Windows Active Directory servers are unclear and inconsistent.
536211	FortiAuthenticator should limit FSSO passwords to 15 characters since that is the limit on FortiGate.
532652	Users audit reports are not working on the backup device in an active-active HA cluster.
558790	Unable to assign more than one admin profile to a user.
550800	The **Authentication Activity** widget can display inconsistent information.
548527	User accounts that have been locked due to repeated invalid password attempts cannot be unlocked from the User Lookup page.
544023	Importing MD5-hashed certificates for system access causes Apache to crash repeatedly.
543646	When creating a password policy, entering foreign characters in the "Use non-alphanumeric characters in random passwords" field will cause an error to occur when viewing the list of guest users.
540587	Clicking on a guest user on a load-balancing device causes a GUI crash.
490281	FortiAuthenticator logs show the column name "Type id", however downloaded logs and logs sent to FortiAnalyzer show this column name as "Log id".
557762	In an active-active HA configuration, after an HA password change, backup devices are unable to synchronize.
557771	The role of active-passive cluster standby member locks to standby member if the active member shuts down while status is "in_sync = 0".
551706	Load-balancing HA clusters are unable to have two remote FortiAuthenticator administrators with the same username when two-factor authentication is enabled.
516357	Toggling load-balancing off and back on in an existing cluster can impact availability for hours or days.
543729	RADIUS Client service not working after upgrading firmware from version 4.2.1 to version 5.5.
548556	If FortiAuthenticator is configured as an LDAP server and the secure password option is enabled, the LDAP client receives an invalid credentials error during the bind attempt.
511093	In an active-active HA configuration, Radiusd on the backup device crashes if a large custom RADIUS dictionary is uploaded to the primary device.
556721	When using the /auth/ REST API endpoint, case insensitivity is ignored when handling the "user has no token configured" option.
543993	Unable to create more than one SSO group using REST API.

Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Feature		Model				
		200E	400E	1000D	2000E	3000E
System						
Network	Static Routes	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20
	SMS Gateways	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20
	User Uploaded Images	39	114	514	1014	2014
	Language Files	50	50	50	50	50
Realms		20	80	400	800	1600
Authentication						
General	Auth Clients (NAS)	166	666	3333	6666	13333
	Users (Local + Remote)[1]	500	2000	10000	20000	40000
	User RADIUS Attributes	1500	6000	30000	60000	120000
	User Groups	50	200	1000	2000	4000
	Group RADIUS Attributes	150	150	600	6000	12000
	FortiTokens	1000	4000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200
	LDAP Entries	1000	4000	20000	40000	80000
	Device (MAC-based Auth.)	2500	10000	50000	100000	200000

Feature		Model				
		200E	400E	1000D	2000E	3000E
	RADIUS Client Profiles	500	2000	10000	20000	40000
	Remote LDAP Servers	20	80	400	800	1600
	Remote LDAP Users Sync Rule	50	200	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	6000	30000	60000	120000
FSSO & Dynamic Policies						
FSSO	FSSO Users	500	2000	10000	20000	200000[3]
	FSSO Groups	250	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	400
	RADIUS Accounting SSO Clients	166	666	3333	6666	13333
	FortiGate Services	50	200	1000	2000	4000
	FortiGate Group Filtering	250	1000	5000	10000	20000
	FSSO Tier Nodes	5	20	100	200	400
	IP Filtering Rules	250	1000	5000	10000	20000
Accounting Proxy	Sources	500	2000	10000	20000	40000
	Destinations	25	100	500	1000	2000
	Rulesets	25	100	500	1000	2000
Certificates						
User Certificates	User Certificates	2500	10000	50000	100000	200000
	Server Certificates	50	200	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50
	Trusted CA Certificates	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	50000	100000	200000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator VM Base License, the number of auth clients (NAS devices) that can authenticate to the system is:

100 / 10 = 10

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666
User Management	**Users**	5	**********	100	5000

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
	(Local + Remote)[1]				
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	RADIUS Client Profiles	3	Users	100	5000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	3	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users /100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	2500	10000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.